Web Application Security

Student number: AB0168
Name: Mays AL-Azzawi
Group: TIC21S
Time management: Approximately 10 hours

Week 04

Insecure Design:

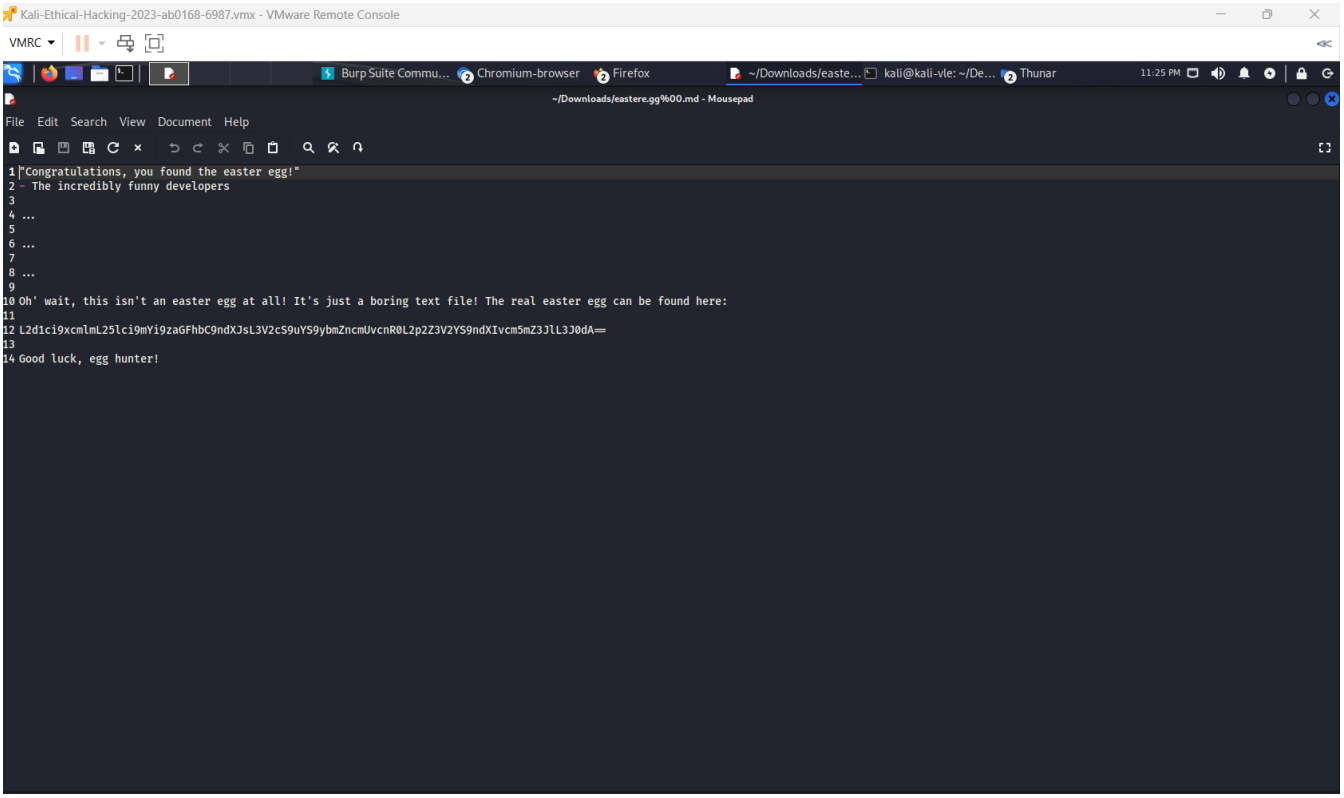
JuiceShop – Easter Egg

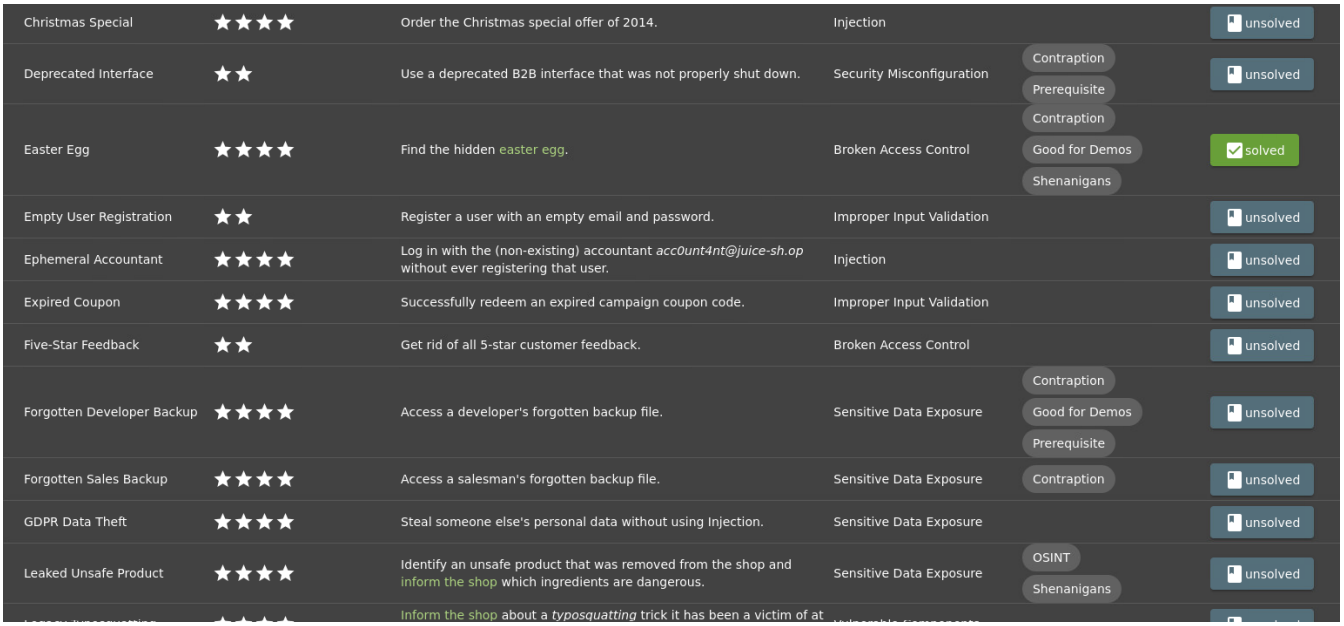
Title: Find Easter Egg from Juice Shop.

Description: Web Application has a file to give instruction about the site and it is work as a robot inside the site and sometimes this file can include a sensitive information or stored password.

Steps to produce:

1. Navigate to `https://wasdat.fi/3000`.
2. Login in to the website.
3. Navigate to `https://wasdat.fi/3000`/robots.txt.
4. The robots.txt file include information allowed to navigate to another page
   user-agent:* ;means applies to all robots
   Disallow: /ftp ; first place to look as it is disallowed
5. In the website : wasdat.fi:3000/ftp. Found an easter.gg file but it is open only as .md file or pdf .
   So navigate to file and add %2500.md
6. The URL : wasdat.fi:3000/ftp/easter.gg%2500.md print a text file which included a further information and got the score.





- Impact estimation:
  - Low Severity: User/robot can identify restricted or confidential information on the site and disallow list can serve as a map to the first place to look.
- Mitigation:
  - Ensure it is correctly configuring, understand the purpose of using robots.txt with your site, create user-agent and test the configuration.

Main target – Coupon codes stored in plain text.

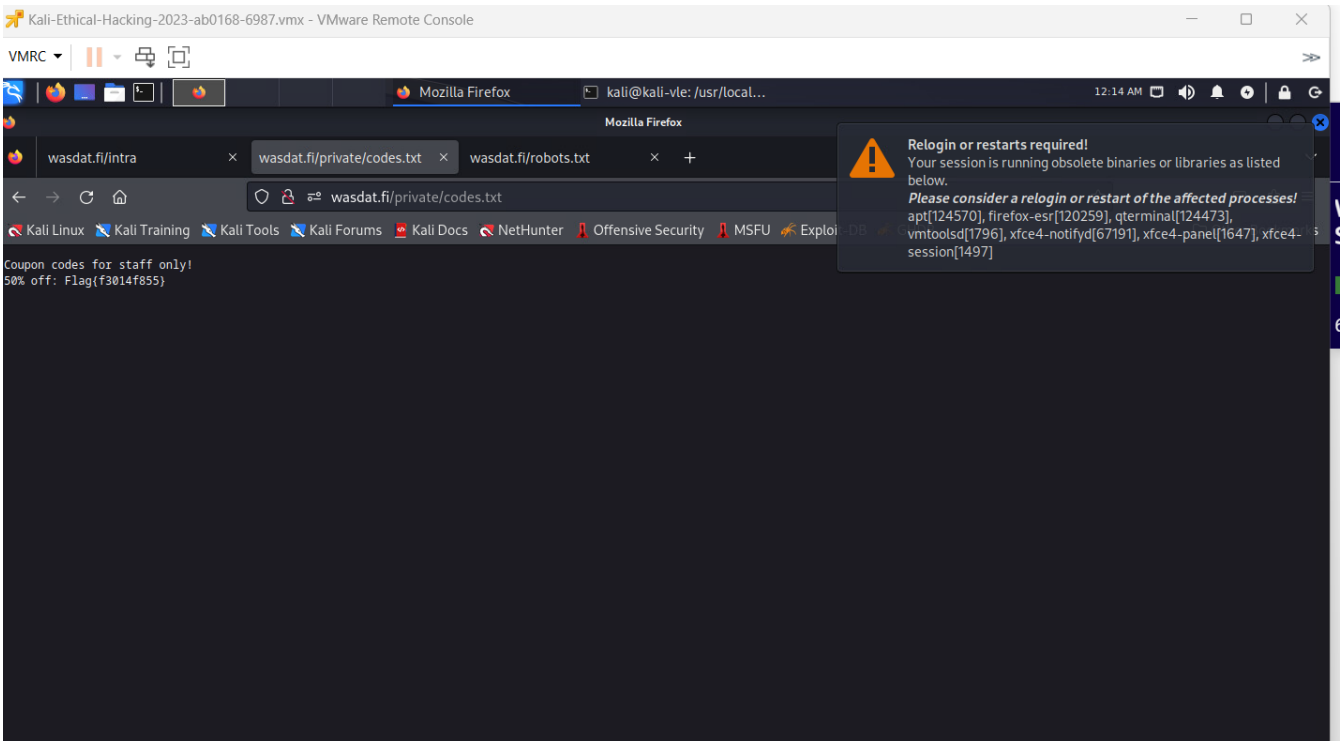
Title: Find and locate a sensitives information containing upcoming coupon codes.

Description: Web Application has a robots.txt file which could include or navigate to sensitive information about the site.

Steps to produce:

1. Navigate to `https://wasdat.fi`.
2. Navigate to the Robots.txt of the wbiste.
   http://Wasdat.fi/robots.txt
3. Inside the robots.txt file there are many disallowed linked which need to look and check .
4. When viewing the URLs found wasdat.fi/private includes two links.
5. Visit the link for codes.txt which may include some information about the code, the text file included the coupon flag.

   Coupon codes for staff only!
   50% off: Flag{f3014f855}



- Impact estimation:
  - High Severity: User/robot can identify restricted or confidential information on the site and disallow list can serve as a map to the first place to look.
- Mitigation:

- Ensure it is correctly configuring, understand the purpose of using robots.txt with your site, create user-agent and test the configuration.

Main target-Login intra :

Title: find and locate intra with a password stored on the target.

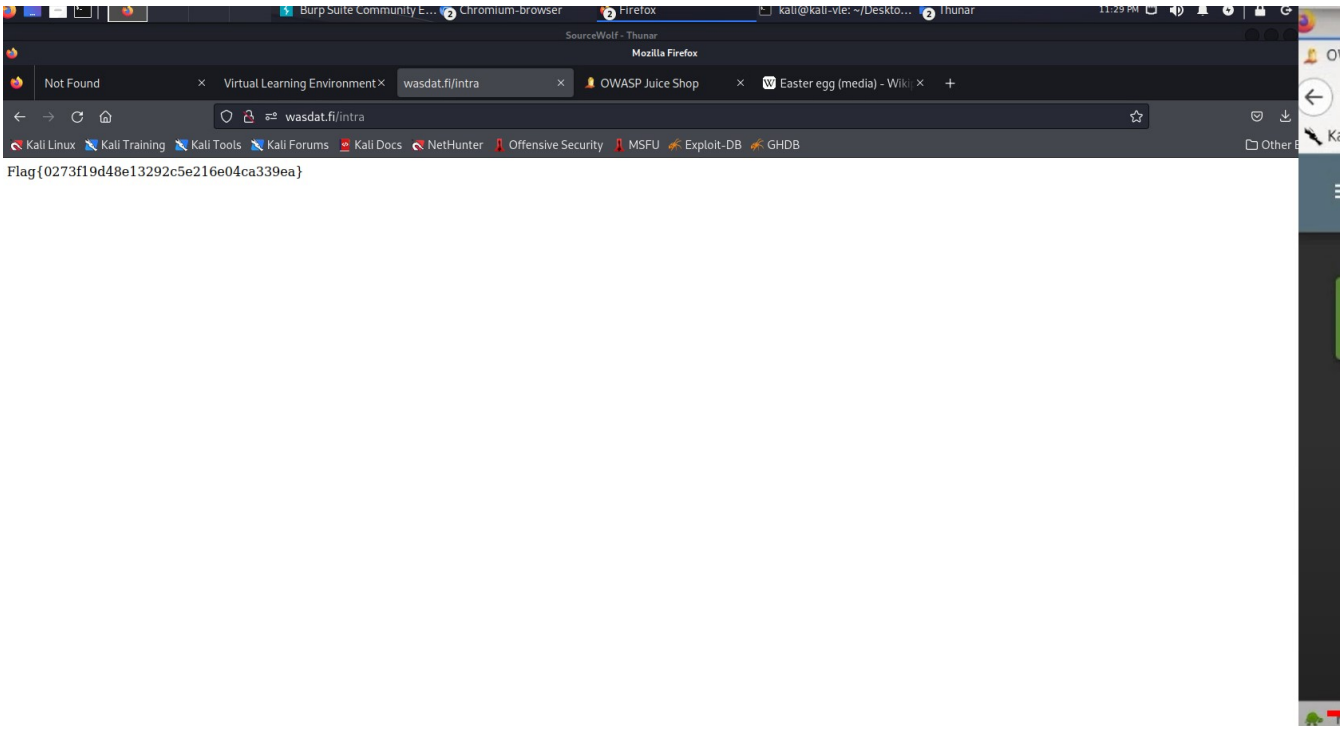
Description: In this task we try to digging deeply for further information we can get from the robots.txt to find a credential information like password to login to intra page.

Steps to produce:

1. Navigate to `https://wasdat.fi`.
2. Navigate to the Robots.txt of the website.
   http://Wasdat.fi/robots.txt
3. Inside the robots.txt file there are many disallowed linked which need to visit and check.
4. When viewing the URLs found
   wasdat.fi/intra: is the intra login page
   wasdat.fi/private : includes two links one of them may have a hidden password in a txt.
5. When clicked on intra-password.conf which may include some credential information as the name describes, the file shows an Error and the page only allowed for .txt files.
6. To open a hidden txt files in the page we add %2500.txt so,
   Wasdat.fi/intra-password.conf%2500.txt.

7. The txt file includes (IntRa-P@sSW0rd-xyz) a sensitive information which we can use later to login to intra page as a password
8. IntRa-P@sSW0rd-xyz used as a password to login to wasdat.fi/intra and the show a flag which navigate to finish our task.

Flag{0273f19d48e13292c5e216e04ca339ea}



- Impact estimation:
  - high Severity:Users enable to find a sensitive information about the credential of the page.
- Mitigation:
  - Understand the use of robots.txt and review the information and the configuration of the website.